Authentication and Isolation of Cryptographic Services for Cloud Computing

Madhavi Shyamsunder Shinde

Abstract**—** Cloud computing is a virtual environment in which resources of the computing infrastructure are providedas data security and access control when users outsource sensitive data for sharing on cloud servers, which are notwithin the same trusted domain as data owners. If a cloud system is responsible for both tasks on storage and encryption/decryption of data, the system administrators may simultaneously obtain encrypted data and decryption keys. This allows them to access information without authorization and thus poses a risk to information privacy. This Project proposes a model for cloud computing based on the concept of separating the encryption and decryption service from the storage service. An authentication method is proposed at a lower level which can be implemented by cloud providers. It is a simple way of authentication which can be utilized by developers along with encryption.

Keywords**—** Cloud computing, encrypted data, authentication, decryption keys etc

I. Introduction

At the present world of networking system, Cloud computing is one the most important and developing concept for both the developers and the users. The cloud offers many strong points: infrastructure flexibility, faster deployment of applications and data, cost control, adaptation of cloud resources to real needs, improved productivity, etc.

Cloud Computing is the result of advancement in the existing technologies. Cloud Computing is beneficial not only for users but also for large and small organizations. Security issues are the major concern in Cloud Computing.

At the present world of networking system, Cloud computing is one the most important and developing concept for both the developers and the users. In the cloud environment, resources are shared among all of the servers, users and individuals. As a result files or data stored in the cloud become open to all. Therefore, data or files of an individual can be handled by all other users of the cloud. Thus the data or files become more vulnerable to attack. As a result it is very easy for an intruder to access, misuse and destroy the original form of data. An intruder can also interrupt the communication. Hence, it is extremely essential for the cloud to be secure. Another problem with the cloud system is that an individual may not have control over the place where the data needed to be stored. A cloud user has to use the resource allocation and scheduling, provided by the cloud service provider. In our proposed security model we have tried to take into account the various security breaches as much as possible.

If a cloud system is answerable for both the tasks on storage and encryption-decryptionof data, the system administrators may concurrently obtain encrypted data and decryption keys and there may be thechances of unauthorized disclosure of data. This allows them to access information without authorization and thusposes a risk to information privacy.

II. Objective

Cloud computing security issues

As cloud computing providing the security there has some issues related to security they are as follows:

A. Security

Security is generally a desired state of being free from harm. As defined in information security, it is a condition in which an information asset is protected against its confidentiality, integrity and availability in the desired state and at the right time.

Professional hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft .

B. Privacy

Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems.

C. Reliability

Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing.

D. Legal Issues

As with other changes in the landscape of computing, certain legal issues arise with cloud computing, including trademark infringement, security concerns and sharing of proprietary data resources.

E.Performance interference and noisy neighbor

Due to its multi-tenant nature and resource sharing, cloud computing must also deal with the "noisy neighbor" effect. This effect in essence indicates that in a shared infrastructure, the activity of a virtual machine on a neighboring core on the

Madhavi Shyamsunder Shinde, M.Tech Student, Department of CSE, JD College of Engineering, Nagpur. (Email: madhavisshinde@gmail.com)

same physical host may lead to increased performance degradation of the VMs in the same physical host, due to issues

However, Cloud Computing has some security issues such as virtualization technology security, massive distributed processing technology, service availability, massive traffic handling, application security, access control, and authentication and password. User authentication among them requires a high-guaranteed security.

Along with authentication of user and all other parties involved in the process of data storing, encrypting, decrypting and retrieving another major goal of this project is securing the cloud by isolating the processes of encryption and decryption. This can be done when encryption and decryption will be done separately by different vendors. In this way the keys used for encryption and decryption will be kept secret. The processes will be in control and there will not be much threat to the security.

III. Literature review

Cloud Computing Business Model: Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud shaped symbol as an abstraction for the complex infrastructure it contains in system. Cloud computing entrusts remote services with a user's data, software and computation.

Services by cloud computing over the network are:

A. PaaS- In this type of service, Platform is provided to the cloud consumer as a service. For example-Operating System.

B. IaaS- In this type of service, infrastructure is provided to the cloud consumer as a service. For example-Storage area, server physical equipment.

C. SaaS- In this type of service, Software is provided to the cloud consumer as a service. For example-Microsoft Word, Notepad, Paint, or many other applications.

In the last decade, much development has taken place in the field of authentication models. A number of frameworks, models and architectures have been proposed by researchers.

This Project proposes a business model for cloud computing based on the concept of separating the encryption and decryption service from the storage service. We take a holistic view of cloud computing through authentication and encryption.

IV. Problem definition

This section addresses the core theme of this chapter, i.e., the security and privacy-related challenges in cloud computing. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure.

For securing data at rest, cryptographic encryption mechanisms are certainly the best options. The hard drive manufacturers are now shipping self-encrypting drives that implement trusted storage standards of the trusted computing group. These self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Although software encryption can also be used for protecting data, it makes the process slower and less secure since it may be possible for an adversary to steal the encryption key from the machine without being detected.

Encryption is the best option for securing data in transit as well. In addition, authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit. Strong authentication is a mandatory requirement for any cloud deployment. User authentication is the primary basis for access control. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. When a user’s access privilege is revoked or reassigned, the customer’s identity management system can notify the cloud provider in real-time so that the user’s cloud access can be modified or revoked within a very short span of time.

V.Research methodology

With the growing popularity of cloud, companies are investing heavily in the research of cloud computing security. In this paper some of the significant and latest research is included which mainly focus on the authentication phase of cloud security. After the thorough review of literature in cloud computing authentication, some new directions and approaches are set forth that can facilitate the researchers in this area.

RSA is Public-Key algorithm. It has been developed by Ron Rivest, Adi Shamir and Len Adleman in 1977. We use RSA algorithm to encrypt the data so that no unauthorized user access it. It provides security of data in cloud. User data is first encrypted and then it is stored in the Cloud. When data is required by user Cloud provider authenticates the user and then delivers the data. RSA is like a block cipher, where every message is mapped to an integer. It consists of Public-Key and Private-Key. Public-Key is known to all, but Private Key is known only to the user who owns the data. Therefore, encryption is done by Cloud service provider and decryption is done by the Cloud user. When the data is encrypted with help of Public-Key, it can only be decrypted with the corresponding Private-Key. RSA algorithm involves three stages: 1. Key Generation 2. Encryption 3. Decryption

Starting with identification of the research problems and studying related solutions, existing technologies and standards, the research goals are defined. Then designing stage goes after, which leads to the preliminary solution for the entire research problem. Afterwards, prototype development process will be performed. During the development stage several modifications and improvements can be introduced, as per the changes in requirements and specifications. System design and prototype development will be followed by testing and deployment stage. Deployment step resulted in collecting several outcomes form system functionality point of view. Finally, analysis and evaluation will be performed from theoretical and practical points of view and further improvements and suggestions will be presented for future work.

VI. OUTCOME

The paper witnesses the evolution of authentication. It shows the development from the usage of hardware tokens to authenticate the client (user). Research is still in progress finding new methods and schemes to authenticate the user in order to challenge the security threats faced by the Cloud. These new approaches by various researchers offer a good foundation for further research and development in the field of Cloud security.

Here we are focusing on the security goal by enhancing the authenticity of the client along with the vendor responsible for encryption and the vendor responsible for decryption process, since there cryptographic processes will be done separately to reduce the risk of misusing the information of decryption key that will be used. Hencewise, more security will be provided to the cloud environment.

VII. CONCLUSION

Three services are provided by cloud Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud service can be accessed by a device that can access the internet.

If storage and encryption/ decryption are provided by a single service provider than there may be a more chances for unauthorized access of data from high level authority like System administers, as he has access to Decryption key and encrypted data that is stored. This paper proposes a Secured cloud computing model based on separating the cloud computing services into two different service providers. The main aim of this paper is dividing of authority to reduce operational risk due to which unauthorized access of data.

Cloud Computing is still an evolving paradigm where computing is on-demand service. Once the organization moves to the cloud, it faces many security issues. Thus, the amount of protection needed to secure data in cloud is directly proportional to the value of the data stored. Security of the Cloud can be improved by trusted computing and cryptography. Thus, in our proposed work, we used RSA algorithm to provide security where only the authorized user can access the data. Even if some unauthorized user gets the data accidentally or intentionally and he captures it, he cannot decrypt it and get back the original data from it.

REFERENCES

[1] Authentication and encryption in Cloud ComputingPublished in: Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference ,Date of Conference: 6-8 May 2015 ,Print ISBN: 978-1-4799-9854-8 , INSPEC Accession Number:15403341, Conference Location:Chennai, DOI:10.1109/ICSTM.2015.7225417, Publisher:IEEE, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7225417&punumber%3D7193753%26filter%3DAND(p_IS_Number%3A7225373)%26pageNumber%3D2

[2] Review on A Business Model for Cloud Computing Based on aSeparate Encryption and Decryption ServiceGaurav Sinha Thakur1, V Kala21M. Tech Scholar, 2Assistant Professor, Department of Computer Science & Engineering, Maharashtra Institute of Technology(MIT), Aurangabad, Maharashtra, IndiaInternational Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 12, December2014)http://www.ijetae.com/files/Volume4Issue12/IJETAE_1214_69.pdf

[3] BUSINESS MODEL BASED ON A SEPARATE ENCRYPTION &DECRYPTION SERVICES FOR CLOUD COMPUTING, 1A. R. KAMBLE, 2SANKET TARAL, 3PRASAD KUBADE, 4ABHISHEK WAGH, 5NIKHIL SHETE, Sinhgad Institute of technology and Science, Narhe, Pune 41, University of Pune, Maharashtra, India, International Journal of Advances in Computer Science and Cloud Computing, ISSN: 2321-4058 Volume- 1, Issue- 2, and Nov-2013, http://iraj.in/journal/journal_file/journal_pdf/5-31-139037364412-15.pdf

[4] A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service, Authors: Jing-Jang Hwang, Hung-Kai Chuang, Yi-Chang Hsu, Chien-Hsing Wu , Published in: · Proceeding ICISA '11 Proceedings of the 2011 International Conference on Information Science and Applications Pages 1-7 , IEEE Computer Society Washington, DC, USA ©2011 ,Table of contents ISBN: 978-1-4244-9222-0 doi>10.1109/ICISA.2011.5772349, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5772349

[5] Data Security in Cloud Computing Using Separate Encryption/Decryption Cloud Service, Authors: Prajakta R Rajapure Dept. of Computer Engineering PES's Modern College of Engineering Pune, India.Swati N Ranpise Dept. of Computer Engineering PES's Modern College of Engineering Pune, India. Deepali S Khandzode Dept. of Computer Engineering PES's Modern College of Engineering Pune, India. Meghana R Kanthale Dept. of Computer Engineering PES's Modern College of Engineering Pune, India , International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 2 Issue: 4 743 – 746

[6] CLOUD COMPUTING A CRM SERVICE BASED ON SEPARATE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM , Rajiv R Bhandari M-Tech Student, Department of IT NRI Institute of Information Science and Technology Bhopal, (MP) India. rajivbhandari@ymail.com Prof.Nitin Mishra Professor, Department of IT NRI Institute of Information Science and Technology Bhopal, (MP) India. nitin.nriist@gmail.comInternational Journal on Recent and Innovation Trends in Computing and Communication Volume: 1 Issue: 4

[7] International Journal of Computer Applications (0975 – 8887) Volume 39– No.18, February 2012 23 the Comprehensive Approach for Data Security in Cloud Computing: A Survey Nilesh N. Kumbhar Virendrasingh V. Chaudhari Mohit A.Badhe

[8] SECURING USER AUTHENTICATION USING SINGLE SIGN-ON IN CLOUD COMPUTING, PUBLISHED IN:ENGINEERING (NUICONE), 2011 NIRMA UNIVERSITY INTERNATIONAL CONFERENCE ONDATE OF CONFERENCE:8-10 DEC. 2011, PRINT ISBN:978-1-4577-2169-4, INSPEC ACCESSION NUMBER:12571758, CONFERENCE LOCATION:AHMEDABAD, GUJARAT, DOI:10.1109/NUICONE.2011.6153227,PUBLISHER:IEEE

[9] Secure user authentication in cloud computing management interfaces, Soares, L.F.B. Dept. of Computer. Sci., Univ. of Beira Interior,Covilha,Portugal Fernandes, D.A.B. ; Freire, M.M. ; Inacio, P.R.M., Published in:Performance Computing and Communications Conference (IPCCC), 2013 IEEE 32nd International, Date of Conference:6-8 Dec. 2013, Print ISBN:978-1-4799-3213-9, INSPEC Accession Number:14117379, Conference Location: San Diego, CA, DOI:10.1109/PCCC.2013.6742763, Publisher:IEEE

[10] Privacy Protection in Cloud Using RSAAlgorithm Amandeep Kaur, Manpreet KaurAmandeep Kaur et al Int. Journal of Engineering Research and Applications , www.ijera.com ISSN: 2248-9622, Vol. 4, Issue 5 (Version 3), May 2014, pp.119-122